Implementation of Security in Wireless Sensor Network using Blowfish Algorithm

S. Pon Priyadharshini
P.G Scholar
National Engineering College,
Kovilpatti

N. Arumuagam
Associate Professor (SG)
National Engineering College,
Kovilpatti

K.SangeethaAnanthamani
Associate Professor (SG)
National Engineering College,
Kovilpatti

ABSTRACT

Wireless Sensor networks are used in wide range of applications such as military sensing and tracking, health monitoring, temperature monitoring, and other areas. Security services are critical in sensor networks. This security, enables the sensor nodes to transmit and receive the sensor values over the network, securely. Here, three sensors LM35, MQ6, LDR sensor are used the values are observed and shown in display. The values are transmitted securely using Atmega8L microcontroller and Zigbee module. In our paper, Blowfish algorithm is used which provides high data confidentiality. The proposed system improves the network security compared to the existing algorithm. The proposed system is implemented and simulated using Proteus software.

General Terms

Wireless Sensor Network (WSN), Security, Blowfish Algorithm.

Keywords

Sensor, Microcontroller, Zigbee

1. INTRODUCTION

Wireless Sensor Network refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. A node is composed of Microcontroller, several sensors, a battery, and Communication modules. WSN measure the Environmental conditions like Temperature, Sound, Pollution levels, Humidity, Wind speed and direction, Pressure, etc. We can choose any kind of sensor for a specific purpose. The working process of sensor network is classified into three parts they are, send any value, using any protocol, to any system. We can sense any kind of value measured from sensor, in second case , we can use any kind of protocol or algorithm to communicate the information and finally we have external system in order to show the data.

WSN have many applications in military, homeland security and other areas. In that many sensor networks have mission critical tasks. Security is critical for such networks deployed in hostile environments[5] [11] [14] [12]. Most sensor networks actively monitor their surroundings, and it is often easy to deduce information other than the data monitored[13]. Such unwanted information leakage often results in privacy breaches of the people in environment. Sensor nodes use wireless communication, easy to eavesdrop. Attacker can easily inject malicious message into network. Anti-jamming and physical temper proofing techniques are impossible due to greater design complexity and energy consumption.

A sensor network is a special type of network. It shares some commonalities with a typical computer network, but also poses unique requirements. Therefore, the requirements of a wireless sensor network as encompassing both the typical network requirements and the unique requirements suited solely to wireless sensor networks. The Security requirements of WSN are Data confidentiality, Authentication, Data Integrity, Data Freshness. Cryptography is a study of secret(crypto-) and writing (-graphy). It is the science or art of encompassing the principles and methods transforming message in to some coded form and then transforming that coded message back to its original form. They are categorised into mainly two types depending upon the type of security keys. The two category are symmetric and asymmetric encryptions. In symmetric or else private encryption only one key is used to encrypt or decrypt the data[4] [3] [15]. The Strength of the symmetric encryption depends upon the size of the key. For the unchanged algorithm, encryption using the longer key is tough to break than one using smaller key [10]. Blowfish is block cipher 64-bit block that can be used as a replacement for the DES algorithm. It takes a variable length key, range from 32 bits to 448 bits; default 128 bits. Blowfish is unpatented, license-free, and is available free for all users.It is best when comparing to the popular existing algorithms.

2. PROPOSED SYSTEM

The proposed method consists of both Transmitter and receiver part.

2.1 Transmitter Block Diagram

Three sensors are used here LM35, MQ6, LDR. LM35 is Temperature Sensor. It is used to observe the room temperature values. MQ6 is Gas Sensor. It is used to sense LPG concentrations in the air. LDR is Light Dependent Resistor. Light Dependent Resistor is a component that has a resistance which changes with the light intensity that falls on it. Fig.1 shows the transmitter diagram.

The before encrypted values will be displayed in the Display Unit. Here, Atmega 8L is used. The Atmega microcontroller is used to encrypt the sensor values. It consists of UART. After encryption, the values will be sent to receiver mode by using the Zigbee Module CC2500.

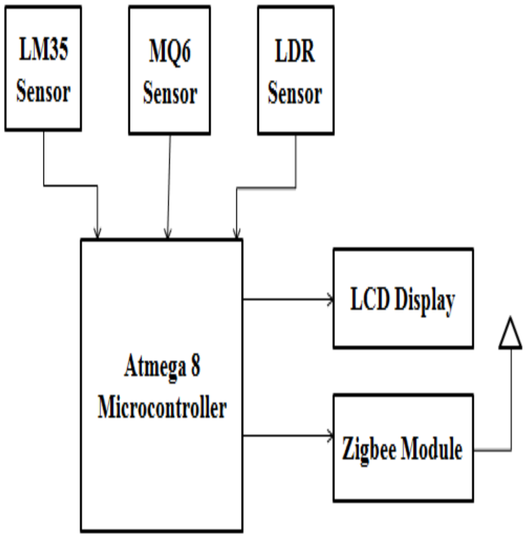


Fig.1 Functional Diagram of Transmitter

2.2 Receiver Block Diagram

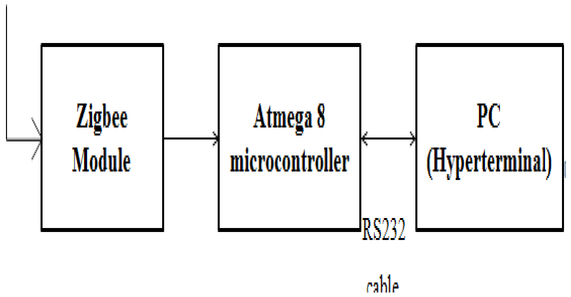


Fig. 2 Functional Diagram of Receiver

The encrypted values are obtained by Receiver mode. Fig.2 shows the Receiver diagram. The Zigbee module receives the encrypted values and then it now decrypted by using the microcontroller by using the same Blowfish algorithm. The System and receiver mode is connected by using RS 232 cable. The original data will be displayed in the PC Hyperterminall

3. SYSTEM DESCRIPTION

3.1 Atmega8 Microcontroller

It is a modified Harvard architecture 8-bit RISC single chip microcontroller which was developed by Atmel in 1996. The AVR was one of the first microcontroller families to use on-chip flash memory for program storage, as opposed to one-time programmable ROM, EPROM, or EEPROM used by other microcontrollers at the time.

Fig.3 Atmega8L microcontroller

3.2 Temperature Sensor

There are a wide variety of temperature sensors on the market today, including Thermocouples, Resistance Temperature Detectors (RTDs), Thermistors, Infrared, and Semiconductor Sensors. This paper will discuss three of these alternatives: the RTD, thermistor, and semiconductor sensors. The LM35 series are precision integrated-circuit temperature sensors, whose output voltage is linearly proportional to the Celsius (centigrade) temperature.

3.3 Gas Sensor

This is a simple-to-use liquefied petroleum gas (LPG) sensor, suitable for sensing LPG (composed of mostly propane and butane) concentrations in the air. The MQ6 can detect gas concentrations anywhere from 200 to 10000ppm. This sensor has a high sensitivity and fast response time. The sensor's output is an analog resistance. Sensitive material of MQ-6 gas sensor is SnO which with lower conductivity in clean air. It make detection by method of cycle high and low temperature, and detect CO when low temperature (heated by 1.5V). The sensor's conductivity is higher along with the gas concentration rising. When high temperature (heated by 5.0V), it cleans the other gases adsorbed under low temperature.

3.4 LDR Sensor

Two cadmium sulphide (cds) photoconductive cells with spectral responses similar to that of the human eye. The cell resistance falls with increasing light intensity. Applications include smoke detection, automatic lighting control, batch counting and burglar alarm systems. LDRs or Light Dependent Resistors are very useful especially in light/dark sensor circuits. Normally the resistance of an LDR is very high, sometimes as high as 1000 000 ohms, but when they are illuminated with light resistance drops dramatically.

3.5 Zigbee Module

ZigBee is a specification for a suite of high level communication protocols used to create personal area networks built from small, low-power digital radios. CC2500 is a FSK /MSK Transceiver module. It provide extensive hardware support for packet handling ,data buffering ,burst transmissions ,clear channel assessment, link quality indication and wake on radio . Its data stream can be Manchester coded by the modulator and decoded by the demodulator .It has a high performance and easily to design your product. It can be used in 2400-2483.5MHz ISM/SRD band systems,Consumer Electronics, Active RFID, Wireless game controllers, wireless KB/Mouse and others wireless systems.

4. BLOWFISH ALGORITHM

Blowfish Algorithm is a Feistal Network , iterating a simple encryption function 16times. The block size is 64 bits, and the key can be any length up to 448 bits[12]. Even though there is a complex initialization phase required before any encryption can take place, the real encryption of data is very efficient on large microprocessors. The Blowfish algorithm is a variablelength key block cipher[6] [3] [8]. It is fit for applications where the key does not change frequently, like a communications link or an automatic file encryptor. It is significantly quicker than most encryption algorithms when implemented on 32-bit microprocessors with large data caches.

4.1 Feistel Network

A Feistel network is a general method of transforming any function (usually called as F function) into a permutation. It was invented by Horst Feistel and has been used in many Block cipher designs.

- Split each block into halves
- Right half becomes new left half
- New right half is the final result when the left half is XOR'd with the result of applying *f* to the right half and the key.
- Note that earlier rounds can be derived even if the function *f* is not invertible.

4.2 Description of Algorithm

Blowfish is a variable-length key, 64-bit block cipher. The algorithm consists of two part: a key-expansion part and a data- encryption part. Key expansion converts a key of at most 448 bits into several subkey arrays totaling 4168 bytes. Data encryption occur via a 16-round Feistel network[10]. Every round consists of a key dependent variation, and a key and data dependent substitution. All operation are XORs and additions on 32-bit words[1] [7] [2]. The only additional operations be four indexed array data lookups per round.

Subkeys

Blowfish uses a large number of subkeys. These keys should be precomputed before any data encryption or decryption.

1. The P-array consists of 18 32-bit subkeys:

P1, P2,.....P18.

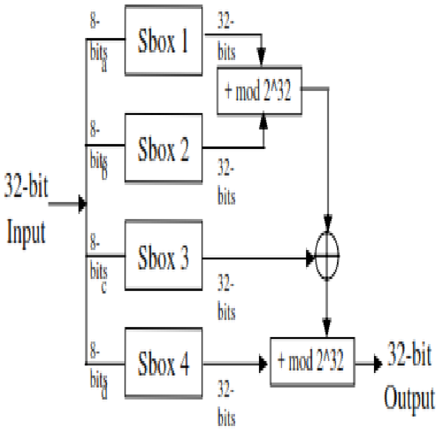
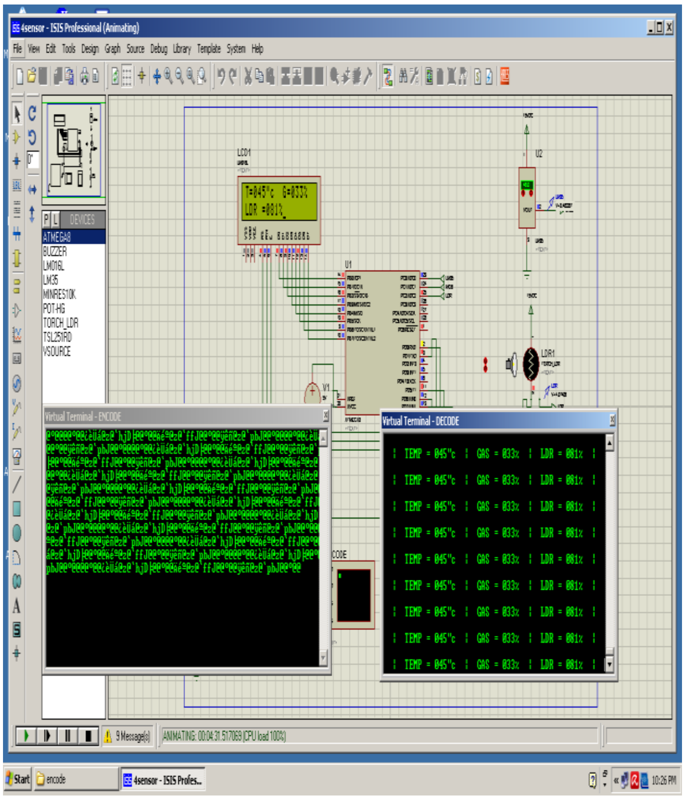


Fig.4 Representation of F function

2. There are four 32-bit S-boxes with 256 entries each:
S1,0, S1,1,...., S1,255;
S2,0, S2,1,..,, S2,255;
S3,0, S3,1,...., S3,255;
S4,0, S4,1,..,, S4,255.
Encryption
1. Blowfish has 16 rounds.
2. The input is a 64-bit data element, x.
3. Divide x into two 32-bit halves: xL, xR.
4. Then, for i = 1 to 16: xL = xL XOR Pi xR = F
5. Swap xL and xR
6. After the sixteenth round, swap xL and xR again to undo the last swap.
Then, xR = xR XOR P17 and xL = xL XOR P18.
7. Finally, recombine xL and xR to get the ciphertext.
8. Decryption is exactly the same as encryption, except that P1, P2,..., P18 are used in the reverse order.
9. Implementations of Blowfish that require the fastest speeds should open the loop and ensure that all subkeys are stored in cache. This figure shows the Blowfish algorithm operation.

5. RESULT AND DISCUSSION

The proposed work is drawn in Proteus software. By clicking the Play option the sensor reading values are shown in the Display .This is the value which shown before encrypt the value.



```
T=045"c  G=033%
LDR =081%_
```

```
¦ TEMP = 045"c ¦ GAS = 033% ¦ LDR = 081% ¦
¦ TEMP = 045"c ¦ GAS = 033% ¦ LDR = 081% ¦
¦ TEMP = 045"c ¦ GAS = 033% ¦ LDR = 081% ¦
¦ TEMP = 045"c ¦ GAS = 033% ¦ LDR = 081% ¦
¦ TEMP = 045"c ¦ GAS = 033% ¦ LDR = 081% ¦
¦ TEMP = 045"c ¦ GAS = 033% ¦ LDR = 081% ¦
¦ TEMP = 045"c ¦ GAS = 033% ¦ LDR = 081% ¦
¦ TEMP = 045"c ¦ GAS = 033% ¦ LDR = 081% ¦
¦ TEMP = 045"c ¦ GAS = 033% ¦ LDR = 081% ¦
```

Fig.5 Simulation Result

The Transmitter diagram is shown in the figure. Three sensors Temperature sensor, Gas sensor, LDR sensor is connected with Amega8L microcontroller. The observed value is shown in the LCD Display. After that it is encrypted and then it is transmitted. The Encrypted values are sent via Zigbee module.

The sensor values are in Analog form. It is then sent to Atmega8 it consists of ADC and UART. The values are observed by microcontroller and some process will takes place. The Encrypted values are sent through Receiver node.

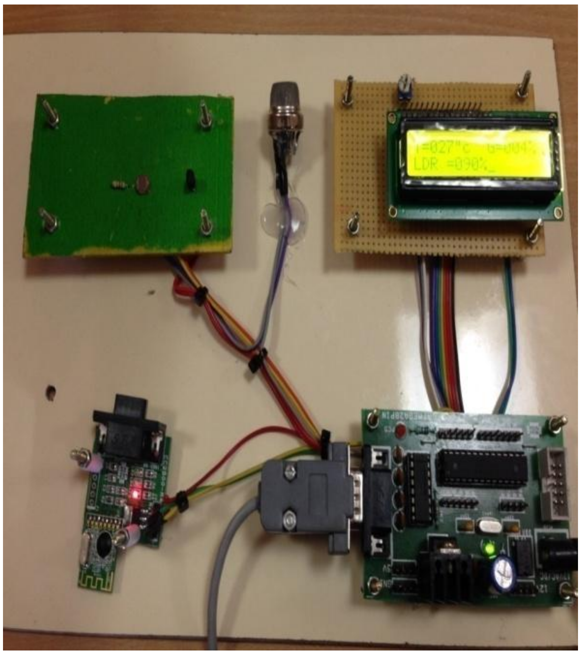


Fig.6 Transmitter node

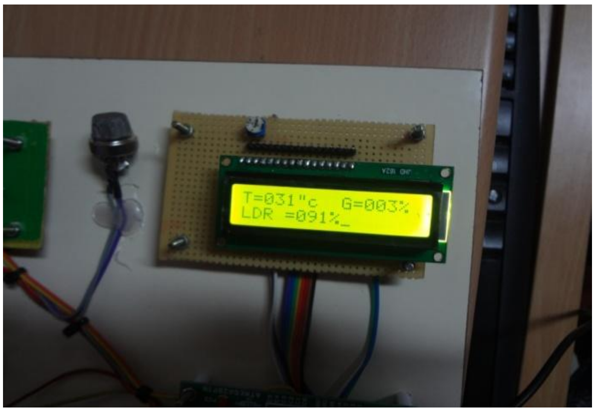


Fig.7 LCD Display

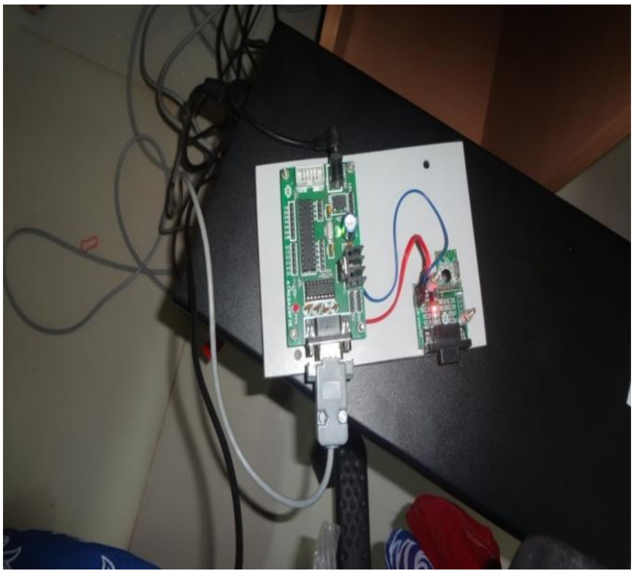
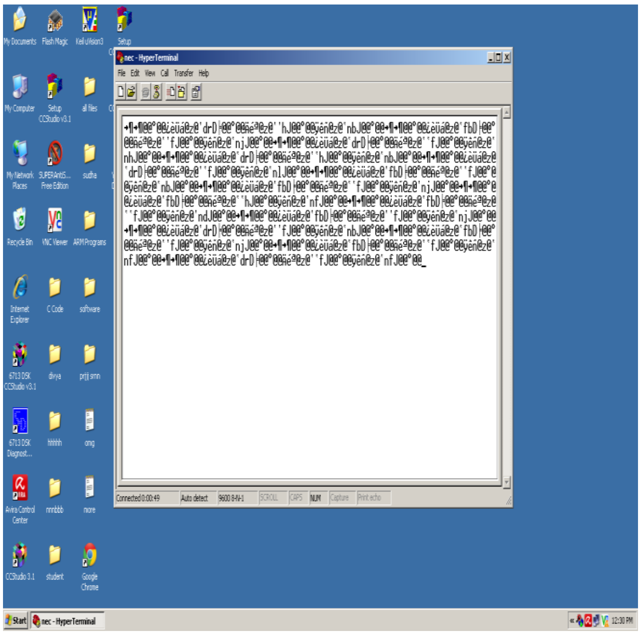
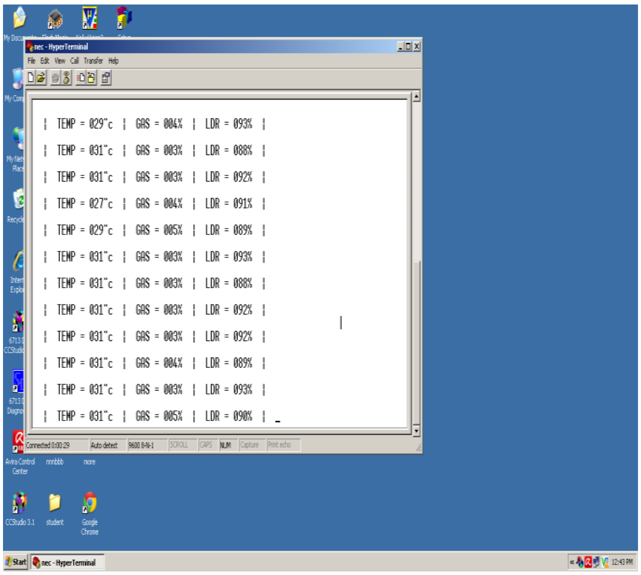


Fig.8 Receiver node



```
→¶→¶@@°@@¿èüá@z@'drD╞@@°@@ñé ª@z@''hJ@@°@@ÿên@z@'nbJ@@°@@→¶→¶@@°@@¿èüá@z@'fbD╞@@°
@@ñé ª@z@''fJ@@°@@ÿên@z@'njJ@@°@@→¶→¶@@°@@¿èüá@z@'drD╞@@°@@ñé ª@z@''fJ@@°@@ÿên@z@'
nhJ@@°@@→¶→¶@@°@@¿èüá@z@'drD╞@@°@@ñé ª@z@''hJ@@°@@ÿên@z@'nbJ@@°@@→¶→¶@@°@@¿èüá@z@
'drD╞@@°@@ñé ª@z@''fJ@@°@@ÿên@z@'nlJ@@°@@→¶→¶@@°@@¿èüá@z@'fbD╞@@°@@ñé ª@z@''fJ@@°@
@ÿên@z@'nbJ@@°@@→¶→¶@@°@@¿èüá@z@'fbD╞@@°@@ñé ª@z@''fJ@@°@@ÿên@z@'njJ@@°@@→¶→¶@@°@
@¿èüá@z@'fbD╞@@°@@ñé ª@z@''hJ@@°@@ÿên@z@'nfJ@@°@@→¶→¶@@°@@¿èüá@z@'fbD╞@@°@@ñé ª@z@
''fJ@@°@@ÿên@z@'ndJ@@°@@→¶→¶@@°@@¿èüá@z@'fbD╞@@°@@ñé ª@z@''fJ@@°@@ÿên@z@'njJ@@°@@
→¶→¶@@°@@¿èüá@z@'drD╞@@°@@ñé ª@z@''fJ@@°@@ÿên@z@'nbJ@@°@@→¶→¶@@°@@¿èüá@z@'fbD╞@@°
@@ñé ª@z@''fJ@@°@@ÿên@z@'njJ@@°@@→¶→¶@@°@@¿èüá@z@'fbD╞@@°@@ñé ª@z@''fJ@@°@@ÿên@z@'
nfJ@@°@@→¶→¶@@°@@¿èüá@z@'drD╞@@°@@ñé ª@z@''fJ@@°@@ÿên@z@'nfJ@@°@@_
```

Fig.9 Encrypted Value



```
¦ TEMP = 029"c ¦ GAS = 004% ¦ LDR = 093% ¦

¦ TEMP = 031"c ¦ GAS = 003% ¦ LDR = 088% ¦

¦ TEMP = 031"c ¦ GAS = 003% ¦ LDR = 092% ¦

¦ TEMP = 027"c ¦ GAS = 004% ¦ LDR = 091% ¦

¦ TEMP = 029"c ¦ GAS = 005% ¦ LDR = 089% ¦

¦ TEMP = 031"c ¦ GAS = 003% ¦ LDR = 093% ¦

¦ TEMP = 031"c ¦ GAS = 003% ¦ LDR = 088% ¦

¦ TEMP = 031"c ¦ GAS = 003% ¦ LDR = 092% ¦

¦ TEMP = 031"c ¦ GAS = 003% ¦ LDR = 092% ¦

¦ TEMP = 031"c ¦ GAS = 004% ¦ LDR = 089% ¦

¦ TEMP = 031"c ¦ GAS = 003% ¦ LDR = 093% ¦

¦ TEMP = 031"c ¦ GAS = 005% ¦ LDR = 090% ¦ _
```

Fig.10 Decrypted Value

The encrypted values are received by Zigbee Module and sent to Atmega microcontroller. Some process will takes place. The encrypted values will be decrypted by the same Blowfish Algorithm. RS 232 cable is connected between system and Receiver node. The encrypted and decrypted values are displayed in the hyperterminal in PC.

Thus the values are transmitted securely by using Blowfish Algorithm.

6. CONCLUSION AND FUTURE WORK

Data encryption is a good means of security but it takes time for their operations to be performed which reduces the speed of data transfer and the capabilities of the network. This can be avoided by implementing properly through hardware or software by using the proposed Algorithm. In this project Blowfish Algorithm is used for implementation of security. Three sensors named as LM35 Temperature sensor, MQ6 Gas sensor, LDR Light Dependent Resistor sensor are used. The values from the sensor are observed by microcontroller Atmega 8 and it will be displayed in the display unit. The values are then encrypted by Atmega microcontroller. The encrypted values are transmitted by using Zigbee module CC2500. The transmitted data's are received by zigbee and the values are decrypted by using Atmega microcontroller. The encrypted and decrypted values are displayed in the hyperterminal in PC. Thus the values are transmitted securely by using the Blowfish Algorithm. In future, this Communication module will be implemented with added features and will be used to send commands to Robot securely mainly in military applications.

7. REFERENCES

[1] Gurjeevan Singh 'Superiority of Blowfish Algorithm in Wireless Networks', International Journal of Computer Applications, April 2012.

[2] Pratibha Rohilla 'Blowfish algorithm: Security and Performance enhancement' , World academy of Informatics and Management Sciences, oct 2012.

[3] Majdi Al qdah, 'Simple Encryption Decryption Application' , Internation Journal of Computer Science and Security, June 2010.

[4] Krishnamurthy, Dr.V.Ramaswamy 'Performance enhancement of Blowfish and CAST-128 algorithms and Security analysis of improved Blowfish algorithm using Avalanchee effect', Intenational Journal of computer Science and Network Security,March 2008.

[5] Simar Preet Singh and Raman Maini 'Comparison of Data Encrytion Algorithms', International Journal of Computer Science and communication, June 2011

[6] M.Anand Kumar 'Investigating the efficiency of Blowfish and Rejindarl algorithms' ,International Journal of computer Network and Information Security,Feb 2012.

[7] Ch Panchamukesh 'An Implementation of Blowfish Encryption algorithm' ,International Journal of Computer Technology and applications, Feb 2011.

[8] Gurjeevan Singh, 'A Study of New trends in Blowfish algorithm' ,Internation Journal of Engineering research and applications, Feb 2011.

[9] C.R. Patel 'FPGA- Hardware Based DES & Blowfish Symmetric cipher algorithm for Encryption and Decryption of Secured wireless Data Communication' ,Journal of Information Knowledge and Research in Electronics and Communication Engineering, Nov 2012.

[10] Encryption Technology White paper, http://security.resist.ca/crypt.htm

[11] Wikipedia,'Encryption', http://en.wikipedia.org/wiki/Encryption, modified on 13 December 2006.

[12] Freeman J., Neely R., and Megalo L. 'Developing Secure Systems: Issues and Solutions'. IEEE Journal of Computer and Communication, Vol. 89, PP. 36-45. 1998

[13] Wikipedia, 'Bitwise operation' http://en.wikipedia.org/wiki/Bitwise_operation, last modified on10 December 2006.

[14] Zainul Abidin, Adharul Muttaqin 'A Simple Cryptography Algorithm for Microcontroller' International Journal of Emerging Technology and Advanced Engineering,2012.

[15] Ali E. Taki El_Deen, 'Microcontroller Application in Cryptography Techniques' Canadian Journal on Electrical and Electronics Engineering Vol. 1, No. 4, June 2010.